PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-187433
(43)Date of publication of application : 21.07.1998

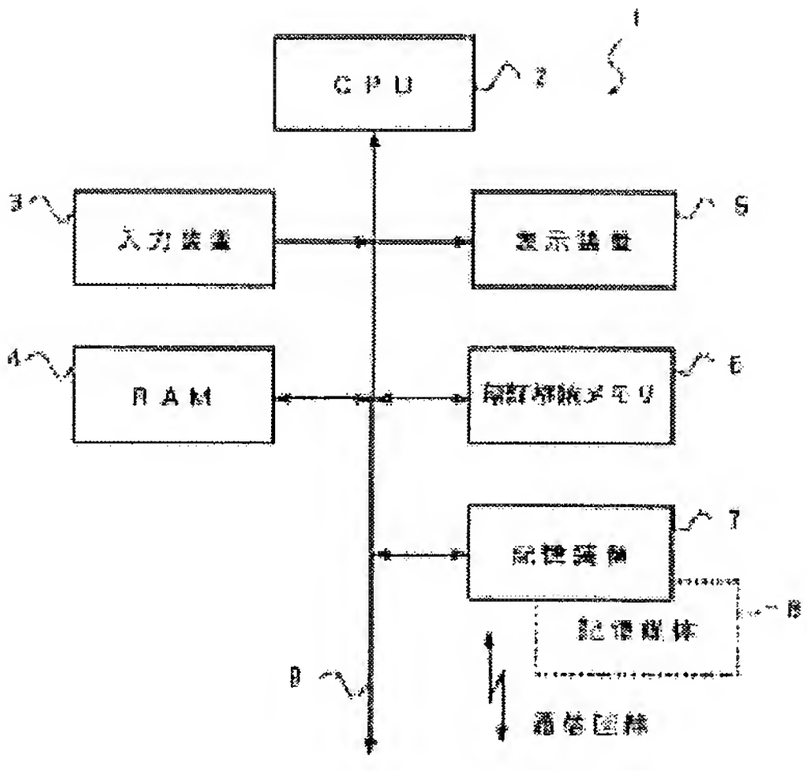
(51)Int.Cl. G06F 9/06
G06F 12/14
// G06F 15/00

(21)Application number : 08-348890
(22)Date of filing : 26.12.1996

(71)Applicant : CASIO COMPUT CO LTD
(72)Inventor : KAYABA YASUSUKE

(54) ELECTRONIC EQUIPMENT AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the illegal copy of software by providing the setting right of password number on the side of system and preventing the contents of password number from being opened for users by providing specified password numbers on the sides of both a storage medium for storing the software and a hardware to install the software and confirming the coincidence of password numbers on both the sides at the time of install.
SOLUTION: When installing an application program(AP) in the case of executing application processing based on an AP, first of all, the coincidence between the password number previously stored in a password storage memory 6 and the password number previously set on the side of that AP is confirmed by a CPU 2 and when the coincidence is confirmed, application processing is continued by judging the user regular but when the password numbers are not coincident, an illegal copy message is displayed on a display device 5 by judging illegal copy so that application processing can be stopped.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－187433

(43)公開日　平成10年(1998)７月21日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｈ
	12/14	３２０		12/14	３２０Ｆ
// Ｇ０６Ｆ	15/00	３３０		15/00	３３０Ｃ

審査請求　未請求　請求項の数４　ＯＬ　（全８頁）

(21)出願番号　特願平8－348890

(22)出願日　平成８年(1996)12月26日

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号

(72)発明者　萱場　庸介
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内

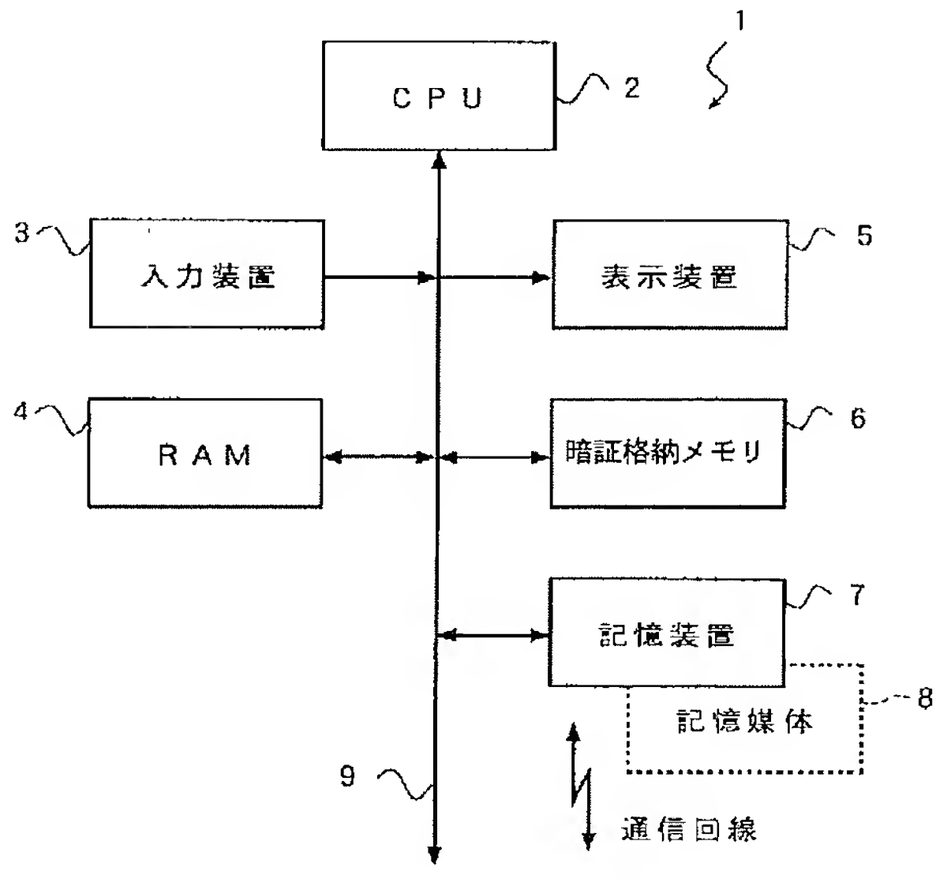
(74)代理人　弁理士　荒船　博司　（外１名）

(54)【発明の名称】　電子機器及び記憶媒体

(57)【要約】

【課題】　ソフトウエアを格納する記憶媒体側とソフトウエアをインストールするハードウエア側との双方で特定の暗証番号を持ち、インストール時に双方で暗証番号の一致を確認することで、暗証番号の設定権限をシステム側に持たせてユーザーには暗証番号の内容を非公開としてソフトウエアの不正コピーを防止することである。

【解決手段】　ＣＰＵ２は、アプリケーションプログラムに基づくアプリケーション処理を実行する際には、アプリケーションプログラムのインストール時に、まず、暗証格納メモリ６に予め格納された暗証番号と、そのアプリケーションプログラム側に予め設定された暗証番号との一致を確認し、一致を確認した場合は正規ユーザーであると判断してアプリケーション処理を続行し、一致しない場合は不正コピーであると判断して不正コピーメッセージを表示装置５に表示して、アプリケーション処理を中止する。



【特許請求の範囲】
【請求項１】アプリケーションプログラムをインストールして利用する電子機器において、
前記アプリケーションプログラムは、固有の暗証情報を設定し、
このアプリケーションプログラムに設定される固有の暗証情報を予め格納した暗証情報記憶手段と、
前記アプリケーションプログラムを実行する際に、当該アプリケーションプログラムに設定された固有の暗証情報と、前記暗証情報記憶手段に格納された固有の暗証情報とを照合することにより、当該アプリケーションプログラムが正規のものか否かを判別する判別手段と、
この判別の結果、前記アプリケーションプログラムが正規のものでないと判別された場合は、当該アプリケーションプログラムの実行を禁止する制御手段と、
を備えたことを特徴とする電子機器。
【請求項２】アプリケーションプログラムをインストールして利用する電子機器において、
前記アプリケーションプログラムは、固有の暗証情報を有し、
このアプリケーションプログラムの固有の暗証情報に対応する暗証情報を記憶する暗証ファイルを有する記憶手段と、
前記アプリケーションプログラムを最初に起動した際に、前記記憶手段内の暗証ファイルの有無及び前記固有の暗証情報を照合する暗証情報照合手段と、
この照合の結果、暗証ファイルが存在し且つ暗証情報が一致した場合は、暗証済情報を設定するとともに前記暗証ファイルを消去し、以降に前記アプリケーションプログラムを起動した際には、前記暗証済情報の設定の有無に基づいて当該アプリケーションプログラムを実行する制御手段と、
を備えたことを特徴とする電子機器。
【請求項３】コンピュータが実行可能なプログラムを格納した記憶媒体であって、
アプリケーションプログラムを実行する際に、当該アプリケーションプログラムに設定された固有の暗証情報と、所定の記憶手段に格納された固有の暗証情報とを照合することにより、当該アプリケーションプログラムが正規のものか否かを判別するためのコンピュータが実行可能なプログラムコードと、
この判別の結果、前記アプリケーションプログラムが正規のものでないと判別された場合は、当該アプリケーションプログラムの実行を禁止するためのコンピュータが実行可能なプログラムコードと、
を含むプログラムを格納したことを特徴とする記憶媒体。
【請求項４】コンピュータが実行可能なプログラムを格納した記憶媒体であって、
アプリケーションプログラムを最初に起動した際に、所定の記憶手段に記憶された暗証ファイルの有無及び前記アプリケーションプログラムに固有の暗証情報との一致を照合するためのコンピュータが実行可能なプログラムコードと、
この照合の結果、暗証ファイルが存在し且つ暗証情報が一致した場合は、暗証済情報を設定するとともに前記暗証ファイルを消去し、以降に前記アプリケーションプログラムを起動した際には、前記暗証済情報の設定の有無に基づいて当該アプリケーションプログラムを実行するためのコンピュータが実行可能なプログラムコードと、
を含むプログラムを格納したことを特徴とする記憶媒体。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ソフトウエアの不正コピーを防止する電子機器及び記憶媒体に関する。
【０００２】
【従来の技術】従来のアプリケーションプログラム等のソフトウエアをインストールして利用するコンピュータシステムにおいて、そのソフトウエアの不正コピーを防止する不正コピー防止方法として、以下に述べるような代表的手法が取られている。
①マスターディスクを特殊なファイル形式でフォーマットし、複製品を作成できないようにする。
②ソフトウエアのインストール時にマスターディスクの内容を書き替え、指定回数以上のコピーができないようにする。
③ソフトウエアのインストール時に、正規ユーザーのみに公開した暗証番号を入力し、暗証番号が一致しない場合はソフトウエアが動作しない、又はインストールの続行ができないようにする。
【０００３】
【発明が解決しようとする課題】しかしながら、このような従来のソフトウエアのコピー防止方法にあっては、マスターディスク又は暗証番号が、エンドユーザーの管理下にあったため、ユーザーのモラル次第で容易に複製品が作成できてしまうという問題があった。
【０００４】すなわち、マスターディスクが特殊なファイル形式でフォーマットされていたとしても、そのフォーマット形式のまま他のディスクにコピーして複製ディスクを作成することは容易であり、また、暗証番号を入力する場合は、正規ユーザーが他者に暗証番号を教えてしまえば、正規ユーザー以外の他者がマスターディスクによりソフトウエアのインストールを行うことは容易である。
【０００５】このため、上記従来の不正コピー防止方法では、正規ユーザーのモラルに頼る部分が多くあり、ソフトウエアを不正コピーから保護する方法としては充分ではなかった。
【０００６】本発明の課題は、ソフトウエアを格納する

記憶媒体側とソフトウエアをインストールするハードウエア側との双方で特定の暗証番号を持ち、インストール時に双方で暗証番号の一致を確認することで、暗証番号の設定権限をシステム側に持たせてユーザーには暗証番号の内容を非公開としてソフトウエアの不正コピーを防止することである。

【０００７】

【課題を解決するための手段】請求項１記載の発明は、アプリケーションプログラムをインストールして利用する電子機器において、前記アプリケーションプログラムは、固有の暗証情報を設定し、このアプリケーションプログラムに設定される固有の暗証情報を予め格納した暗証情報記憶手段と、前記アプリケーションプログラムを実行する際に、当該アプリケーションプログラムに設定された固有の暗証情報と、前記暗証情報記憶手段に格納された固有の暗証情報とを照合することにより、当該アプリケーションプログラムが正規のものか否かを判別する判別手段と、この判別の結果、前記アプリケーションプログラムが正規のものでないと判別された場合は、当該アプリケーションプログラムの実行を禁止する制御手段と、を備えたことを特徴としている。

【０００８】したがって、ソフトウエアを格納する記憶媒体側とソフトウエアをインストールするハードウエア側との双方で特定の暗証番号を持ち、インストール時に双方で暗証番号の一致を確認することで、暗証番号の設定権限をシステム側に持たせてユーザーには暗証番号の内容を非公開とすることができ、他のコンピュータシステムでのアプリケーションプログラムの利用を防止することができ、ユーザーによるソフトウエアの不正コピーを防止することができる。

【０００９】請求項２記載の発明は、アプリケーションプログラムをインストールして利用する電子機器において、前記アプリケーションプログラムは、固有の暗証情報を有し、このアプリケーションプログラムの固有の暗証情報に対応する暗証情報を記憶する暗証ファイルを有する記憶手段と、前記アプリケーションプログラムを最初に起動した際に、前記記憶手段内の暗証ファイルの有無及び前記固有の暗証情報を照合する暗証情報照合手段と、この照合の結果、暗証ファイルが存在し且つ暗証情報が一致した場合は、暗証済情報を設定するとともに前記暗証ファイルを消去し、以降に前記アプリケーションプログラムを起動した際には、前記暗証済情報の設定の有無に基づいて当該アプリケーションプログラムを実行する制御手段と、を備えたことを特徴としている。

【００１０】したがって、ソフトウエア側で特定の暗証番号を含む暗証ファイルを持ち、アプリケーション起動時には、暗証チェック済フラグを確認するだけであり、暗証番号の設定権限をソフトウエア側に持たせたため、ユーザーに暗証番号が知られたとしても、インストール後に暗証番号を入力することを無意味として、不正コピーされたアプリケーションプログラムの利用を防止することができる。

【００１１】

【発明の実施の形態】以下、図を参照して本発明の実施の形態を詳細に説明する。

【００１２】（第１の実施の形態）図１～図３は、本発明の電子機器及び記憶媒体を適用した第１の実施の形態のコンピュータシステムを示す図である。

【００１３】まず、構成を説明する。

【００１４】図１は、本第１の実施の形態のコンピュータシステム１の要部構成を示すブロック図である。この図１において、コンピュータシステム１は、ＣＰＵ２、入力装置３、ＲＡＭ４、表示装置５、暗証格納メモリ６、記憶装置７及び記憶媒体８等により構成されており、記憶媒体８を除く各部はバス９に接続されている。

【００１５】ＣＰＵ（Central Processing Unit）２は、記憶装置７に記憶されているシテムプログラム及び当該システムに対応する各種アプリケーションプログラムの中から指定されたアプリケーションプログラムをＲＡＭ４内の図示しないプログラム格納領域に格納し、入力装置３から入力される各種指示あるいはデータをＲＡＭ４内に格納し、この入力指示及び入力データに応じて記憶装置７内に格納したアプリケーションプログラムに従って各種処理を実行し、その処理結果をＲＡＭ４内に格納するとともに、表示装置５に表示する。そして、ＲＡＭ４に格納した処理結果を入力装置３から入力指示される記憶装置７内の保存先に保存する。

【００１６】また、ＣＰＵ２は、後述するアプリケーションプログラムに基づくアプリケーション処理を実行する際には、アプリケーションプログラムのインストール時に、まず、暗証格納メモリ６に予め格納された暗証番号と、そのアプリケーションプログラム側に予め設定された暗証番号との一致を確認し、一致を確認した場合は正規ユーザーであると判断してアプリケーション処理を続行し、一致しない場合は不正コピーであると判断して不正コピーメッセージを表示装置５に表示して、アプリケーション処理を中止する。

【００１７】入力装置３は、カーソルキー、数字入力キー及び各種機能キー等を備え、押下されたキーの押下信号をＣＰＵ２に出力する。

【００１８】ＲＡＭ（Random Accesss Memory）４は、ＣＰＵ２により処理されるプログラムやデータを一時的に格納するメモリエリアを形成する。表示装置５は、ＣＲＴ（Cathode Ray Tube）等により構成され、ＣＰＵ２から入力される表示データを表示するとともに、上記ＣＰＵ２により実行されるアプリケーション処理に際して入力される不正コピーであることを示すメッセージを表示する。

【００１９】暗証格納メモリ６は、フラッシュメモリ等により構成され、上記ＣＰＵ２によりアプリケーション

処理が実行される際に参照される暗証番号を格納する。この暗証格納メモリ６に格納された暗証番号は、エンドユーザーには非公開で予め格納され、ユーザーによるアクセスを不可とする。

【００２０】記憶装置７は、プログラムやデータ等か予め記憶されている記憶媒体８を有しており、この記憶媒体８は磁気的、光学的記録媒体、若しくは半導体メモリで構成されている。この記憶媒体８は記憶装置７に固定的に設けたもの、若しくは着脱自在に装着するものであり、この記憶媒体８には上記システムプログラム及び当該システムに対応する各種アプリケーションプログラム、暗証番号チェック処理プログラム及び各処理プログラムで処理されたデータ等を記憶する。

【００２１】また、この記憶媒体８に記憶するプログラム、データ等は、通信回線等を介して接続された他の機器から受信して記憶する構成にしてもよく、更に、通信回線等を介して接続された他の機器側に上記記憶媒体を備えた記憶装置を設け、この記憶媒体８に記憶されているプログラム、データを通信回線を介して使用する構成にしてもよい。

【００２２】次に、本第１の実施の形態の動作を説明する。

【００２３】上記ＣＰＵ２により実行されるアプリケーション処理について図２に示すフローチャートに基づいて説明する。

【００２４】ＣＰＵ２は、アプリケーションプログラムが格納された記憶媒体８が記憶装置７にセットされて、そのアプリケーションプログラムをＲＡＭ４にインストールすると、まず、このインストールされたアプリケーションプログラムに予め設定された暗証番号（ＸＸＸＸ…）を読み出し（ステップＳ１）、暗証番号チェックファンクション処理を実行する（ステップＳ２）。

【００２５】この暗証番号チェックファンクション処理の詳細について図３に示すフローチャートに基づいて説明する。

【００２６】図３に示す暗証番号チェックファンクション処理において、アプリケーションプログラムに予め設定された暗証番号（ＸＸＸＸ…）をＲＡＭ４に展開されると、暗証格納メモリ６に格納された暗証番号を読み出し（ステップＳ２１）、そのアプリケーションプログラムに設定された暗証番号と、暗証格納メモリ６から読み出した暗証番号とが一致するか否かを判別する（ステップＳ２２）。暗証番号が一致した場合は、暗証番号が一致した旨の情報を設定して（ステップＳ２３）、図２のステップＳ３に戻り、暗証番号が不一致であった場合は、暗証番号が不一致である旨の情報を設定して（ステップＳ２４）、図２のステップＳ３に戻る。

【００２７】この暗証番号チェックファンクション処理が終了すると、図２のステップＳ３に戻り、暗証番号の一致情報が設定されたか不一致情報が設定されたかをチェックする。暗証番号の一致情報が設定された場合は、正規ユーザーである判断して、アプリケーションプログラムのインストール処理を続行し（ステップＳ４）、暗証番号の不一致情報が設定された場合は、インストールされたアプリケーションプログラムは不正コピーされたものであると判断して、不正コピーであることを示すメッセージを表示装置５に表示する（ステップＳ５）。

【００２８】そして、ステップＳ４におけるアプリケーションプログラムによる処理を終了した後、あるいはステップＳ５における不正コピーメッセージの表示処理を終了した後、本アプリケーション処理を終了する。

【００２９】以上のように、本第１の実施の形態のコンピュータシステム１では、フラッシュメモリから構成された暗証格納メモリ６を備え、この暗証格納メモリ６にはエンドユーザーに非公開の暗証番号を予め格納し、アプリケーション処理を実行する際には、この暗証格納メモリ６に格納された暗証番号と、アプリケーションプログラムに設定された暗証番号との一致を確認することにより、セットされたアプリケーションプログラムが正規ユーザーのものか否かを判断して、そのアプリケーションプログラムを続行するか中止するかをコンピュータシステム１側で判断するようにしたため、不正コピーされた暗証番号の異なるアプリケーションプログラムの実行を回避することができる。

【００３０】したがって、ソフトウエアを格納する記憶媒体側とソフトウエアをインストールするハードウエア側との双方で特定の暗証番号を持ち、インストール時に双方で暗証番号の一致を確認することで、暗証番号の設定権限をシステム側に持たせてユーザーには暗証番号の内容を非公開としたため、他のコンピュータシステムでのアプリケーションプログラムの利用を防止することができ、ユーザーによるソフトウエアの不正コピーを防止することができる。

【００３１】また、暗証格納メモリ６へのユーザーによるアクセスを不可としたため、ユーザーによる暗証番号の取り出しを防止して暗証番号がユーザーに知られることを防止することができ、暗証番号の取得によるアプリケーションプログラムの不正コピーを防止することができる。

【００３２】なお、本第１の実施の形態では、コンピュータシステム１に格納される暗証番号とアプリケーションプログラムに設定された暗証番号が一致することにより、アプリケーションプログラムの実行を可能としたため、そのシステム構成は汎用的なものよりも、例えば、事務処理等の特定の処理を実行するために構成されたコンピュータシステム等に適用することがより有効である。

【００３３】また、本第１の実施の形態では、ソフトウエアの不正コピーを防止するためフラッシュメモリで構成された暗証格納メモリ６に暗証番号を格納するように

したが、その暗証番号の格納場所は、ソフトウエアがインストールされる記憶装置７内のメモリ領域と同一のメモリ領域であっても良く、暗証番号の格納場所は特に限定されるものではない。

【００３４】（第２の実施の形態）図４～図６は、本発明の電子機器及び記憶媒体を適用した第２の実施の形態のコンピュータシステムを示す図である。

【００３５】まず、構成を説明する。

【００３６】図４は、本第２の実施の形態のコンピュータシステム２０の要部構成を示すブロック図である。この図４において、コンピュータシステム２０は、ＣＰＵ２１、入力装置２２、ＲＡＭ２３、表示装置２４、記憶装置２５及び記憶媒体２６等により構成されており、記憶媒体２６を除く各部はバス２７に接続されている。

【００３７】ＣＰＵ（Central Processing Unit）２１は、記憶装置２５に記憶されているシテムプログラム及び当該システムに対応する各種アプリケーションプログラムの中から指定されたアプリケーションプログラムをＲＡＭ２３内の図示しないプログラム格納領域に格納し、入力装置２２から入力される各種指示あるいはデータをＲＡＭ２３内に格納し、この入力指示及び入力データに応じて記憶装置２５内に格納したアプリケーションプログラムに従って各種処理を実行し、その処理結果をＲＡＭ２３内に格納するとともに、表示装置２４に表示する。そして、ＲＡＭ２３に格納した処理結果を入力装置２２から入力指示される記憶装置２５内の保存先に保存する。

【００３８】また、ＣＰＵ２１は、後述するアプリケーションプログラムに基づくアプリケーション処理を実行する際には、ＲＡＭ２３へのアプリケーションプログラムのインストールと同時に暗証ファイルをインストールして、暗証番号をＲＡＭ２３内の暗証ファイルメモリ２３ａと他のメモリエリアに夫々格納し、このインストールしたアプリケーションプログラムの起動時に暗証ファイルの有無及び内容（暗証番号）を照合し、一致した場合にＲＡＭ２３内に暗証チェックフラグ２３ｃをセット（ＯＮ）して、暗証ファイルを消去した後、暗証チェックフラグ２３ｃがセット（ＯＮ）されている時のみアプリケーションプログラムの処理を続行可能とする。

【００３９】入力装置３は、カーソルキー、数字入力キー及び各種機能キー等を備え、押下されたキーの押下信号をＣＰＵ２に出力する。

【００４０】ＲＡＭ（Random Accesss Memory）２３は、ＣＰＵ２１により処理されるプログラムやデータを一時的に格納するメモリエリアを形成するとともに、アプリケーション処理に関わるメモリエリアとして図５に示す暗証ファイルメモリ２３ａ、アプリケーションプログラムメモリ２３ｂ及び暗証チェック済フラグメモリ２３ｃをを形成する。暗証ファイルメモリ２３ａは、上記ＣＰＵ２１によるアプリケーション処理に際してアプリケーションプログラムとともにインストールされる暗証ファイルを格納するために利用され、アプリケーションプログラムメモリ２３ｂは、インストールされるアプリケーションプログラムを格納するために利用される。暗証チェック済フラグメモリ２３ｃは、上記ＣＰＵ２１によるアプリケーション処理に際してインストールされた暗証ファイルによりセットされる暗証内容の照合が一致した際にＯＮされる暗証チェック済フラグを格納するために利用される。

【００４１】表示装置２４は、ＣＲＴ（Cathode Ray Tube）等により構成され、ＣＰＵ２１から入力される表示データを表示するとともに、上記ＣＰＵ２１により実行されるアプリケーション処理に際して入力される不正コピーであることを示すメッセージを表示する。

【００４２】記憶装置２５は、プログラムやデータ等か予め記憶されている記憶媒体２６を有しており、この記憶媒体２６は磁気的、光学的記録媒体、若しくは半導体メモリで構成されている。この記憶媒体２６は記憶装置２５に固定的に設けたもの、若しくは着脱自在に装着するものであり、この記憶媒体２６には上記システムプログラム及び当該システムに対応する各種アプリケーションプログラム、暗証番号チェック処理プログラム及び各処理プログラムで処理されたデータ等を記憶する。

【００４３】また、この記憶媒体２６に記憶するプログラム、データ等は、通信回線等を介して接続された他の機器から受信して記憶する構成にしてもよく、更に、通信回線等を介して接続された他の機器側に上記記憶媒体を備えた記憶装置を設け、この記憶媒体２６に記憶されているプログラム、データを通信回線を介して使用する構成にしてもよい。

【００４４】次に、本第２の実施の形態の動作を説明する。

【００４５】上記ＣＰＵ２１により実行されるアプリケーション処理について図６に示すフローチャートに基づいて説明する。

【００４６】ＣＰＵ２１は、アプリケーションプログラムが格納された記憶媒体２６が記憶装置２５にセットされて、そのアプリケーションプログラムのインストールを開始すると、まず、ＲＡＭ２３内の暗証チェック済フラグメモリ２３ｃに暗証チェック済フラグがセット（ＯＮ）されているか否かをチェックする（ステップＳ３１）。暗証チェック済フラグがセット（ＯＮ）されている場合は、ステップＳ３７に移行してインストールしたアプリケーションプログラムの処理を続行し、暗証チェック済フラグがセットされていない（ＯＦＦ）場合は、ＲＡＭ２３内の暗証ファイルメモリ２３ａ又は他のメモリエリアの夫々に暗証番号が格納されているか否かをチェックする（ステップＳ３２）。

【００４７】ＲＡＭ２３内の暗証ファイルメモリ２３ａ又は他のメモリエリアの夫々に暗証番号が格納されてい

ない場合は、インストールされたアプリケーションプログラムは不正コピーされたものであると判断して、ステップＳ３８に移行して、不正コピーであることを示すメッセージを表示装置２４に表示して、本アプリケーション処理を終了する。また、ＲＡＭ２３内の暗証ファイルメモリ２３ａ又は他のメモリエリアの夫々に暗証番号が格納されている場合は、その各暗証番号を読み出して（ステップＳ３３）、その各暗証番号が一致するか否かをチェックする（ステップＳ３４）。

【００４８】その読み出した各暗証番号が一致しない場合は、ステップＳ３８に移行して、不正コピーであることを示すメッセージを表示装置２４に表示して、本アプリケーション処理を終了する。また、その読み出した各暗証番号が一致した場合は、ＲＡＭ２３内の暗証ファイルメモリ２３ａ又は他のメモリエリアの夫々に暗証番号を削除し（ステップＳ３５）、ＲＡＭ２３内の暗証チェック済フラグメモリ２３ｃに暗証チェック済フラグをセット（ＯＮ）する（ステップＳ３６）。

【００４９】次いで、インストールしたアプリケーションプログラムによる処理を続行し（ステップＳ３７）、そのアプリケーションプログラムによる処理を終了した後、本アプリケーション処理を終了する。

【００５０】以上のように、本第２の実施の形態のコンピュータシステム２０では、アプリケーションプログラムのインストール時に、アプリケーションプログラムにより提供される暗証番号を含む暗証ファイルをＲＡＭ２３内にセットするようにして、上記第１の実施の形態で必要とした暗証格納ファイル６を不要としたため、一般的な構成のコンピュータシステムにも本発明を適用することが可能となる。

【００５１】また、暗証内容の照合後は、その暗証ファイル及び暗証番号を削除して、暗証チェック済フラグのみをチェックして、同一のアプリケーションプログラムの処理を可能としたため、アプリケーションプログラムを一度起動した後に、不正コピーされた暗証ファイルを含むアプリケーションプログラムのインストールを排除することができる。

【００５２】したがって、ソフトウエア側で特定の暗証番号を含む暗証ファイルを持ち、アプリケーション起動時には、暗証チェック済フラグを確認するだけであり、暗証番号の設定権限をソフトウエア側に持たせたため、ユーザーに暗証番号が知られたとしても、インストール後に暗証番号を入力することを無意味として、不正コピーされたアプリケーションプログラムの利用を防止することができる。また、上記第１の実施の形態と同様に他のコンピュータシステムでのアプリケーションプログラムの利用を防止することができ、ユーザーによるソフトウエアの不正コピーを防止することができる。

【００５３】また、インストール終了後は暗証ファイルを消去してしまうため、ＲＡＭ２３内の暗証ファイル２３ａへのユーザーによるアクセスも無意味となり、ユーザーによる暗証ファイルの取り出しを防止して暗証番号がユーザーに知られることを防止することができ、暗証番号の取得によるアプリケーションプログラムの不正コピーを防止することができる。

【００５４】なお、上記第２の実施の形態では、暗証ファイル自体を隠しファイル化したり、暗証ファイルメモリ２３ａを暗号化して、不正コピー対策を強化することも可能である。

【００５５】

【発明の効果】請求項１記載の発明の電子機器及び請求項３記載の発明の記憶媒体によれば、ソフトウエアを格納する記憶媒体側とソフトウエアをインストールするハードウエア側との双方で特定の暗証番号を持ち、インストール時に双方で暗証番号の一致を確認することで、暗証番号の設定権限をシステム側に持たせてユーザーには暗証番号の内容を非公開とすることができ、他のコンピュータシステムでのアプリケーションプログラムの利用を防止することができ、ユーザーによるソフトウエアの不正コピーを防止することができる。

【００５６】請求項２記載の発明の電子機器及び請求項４記載の発明の記憶媒体によれば、ソフトウエア側で特定の暗証番号を含む暗証ファイルを持ち、アプリケーション起動時には、暗証チェック済フラグを確認するだけであり、暗証番号の設定権限をソフトウエア側に持たせたため、ユーザーに暗証番号が知られたとしても、インストール後に暗証番号を入力することを無意味として、不正コピーされたアプリケーションプログラムの利用を防止することができる。

【図面の簡単な説明】

【図１】本発明の電子機器及び記憶媒体を適用した第１の実施の形態のコンピュータシステムの要部構成を示すブロック図。

【図２】図１のＣＰＵ２により実行されるアプリケーション処理のフローチャート。

【図３】図２の暗証番号チェックファンクション処理のフローチャート。

【図４】本発明の電子機器及び記憶媒体を適用した第２の実施の形態のコンピュータシステムの要部構成を示すブロック図。

【図５】図４のＲＡＭ２３内のメモリ構成を示す図。

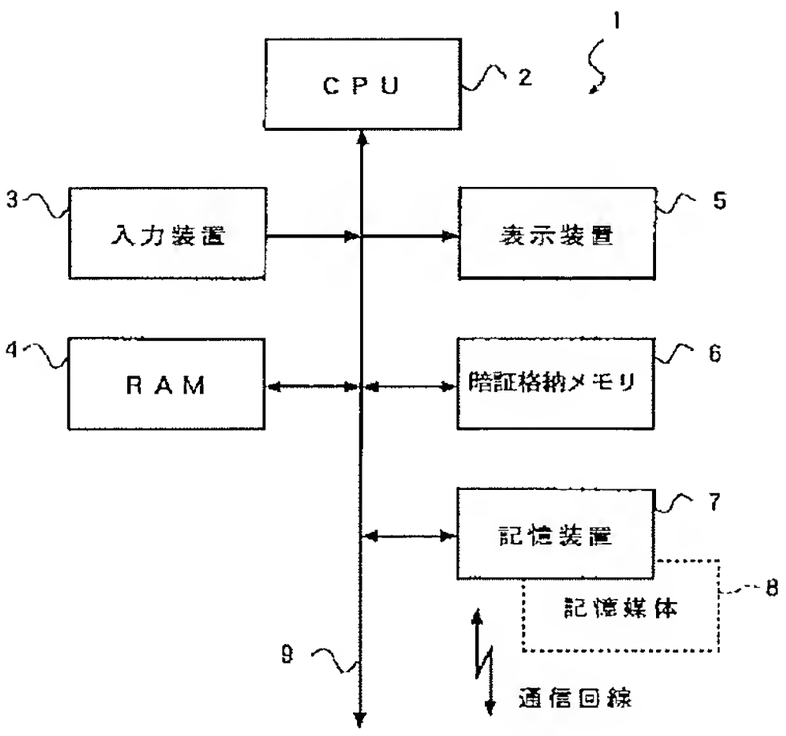
【図６】図４のＣＰＵ２１により実行されるアプリケーション処理のフローチャート。

【符号の説明】

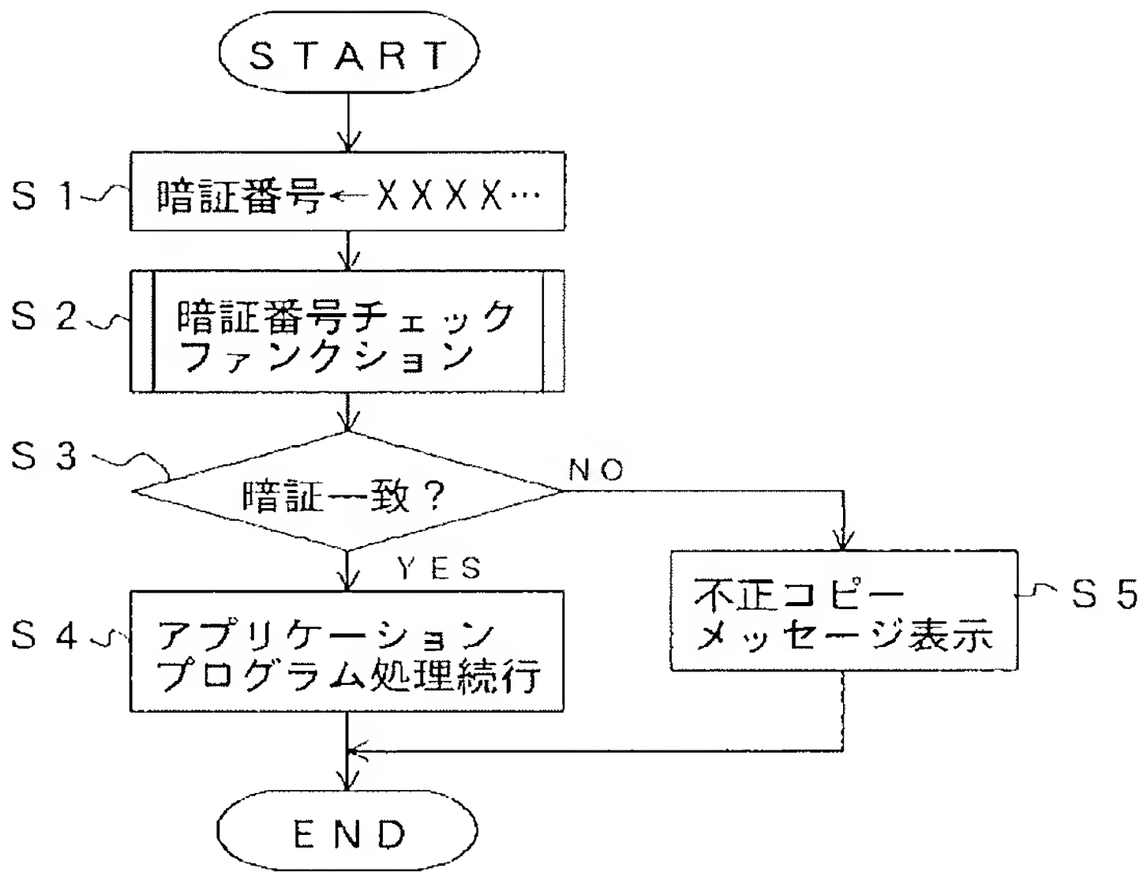
１、２０　コンピュータシステム
２、２１　ＣＰＵ
３、２２　入力装置
４、２３　ＲＡＭ
２３ａ　暗証ファイルメモリ
２３ｂ　アプリケーションプログラムメモリ

２３ｃ　暗証チェック済フラグメモリ
５、２４　表示装置
６　暗証格納メモリ
＊７、２５　記憶装置
８、２６　記憶媒体
＊９、２７　バス

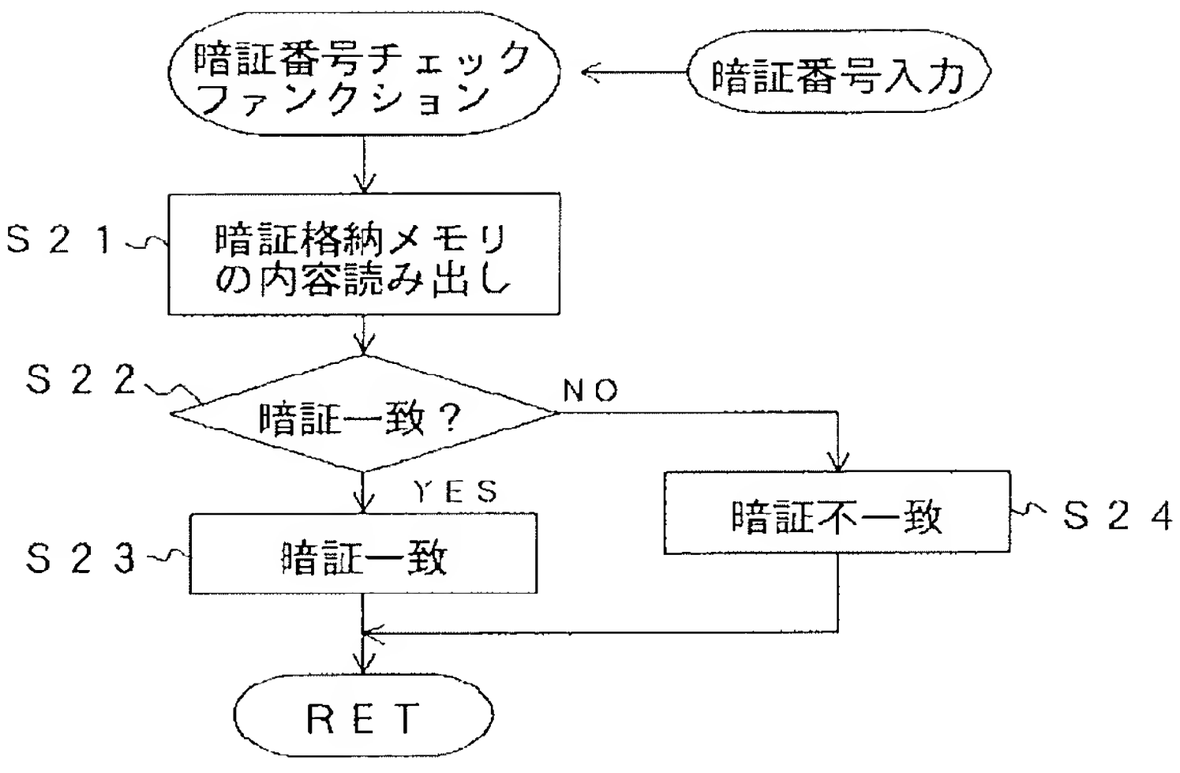
【図１】



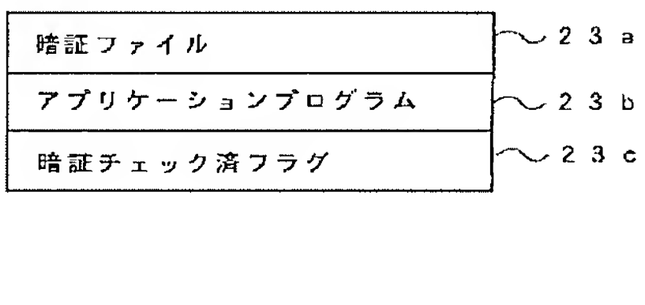
【図２】



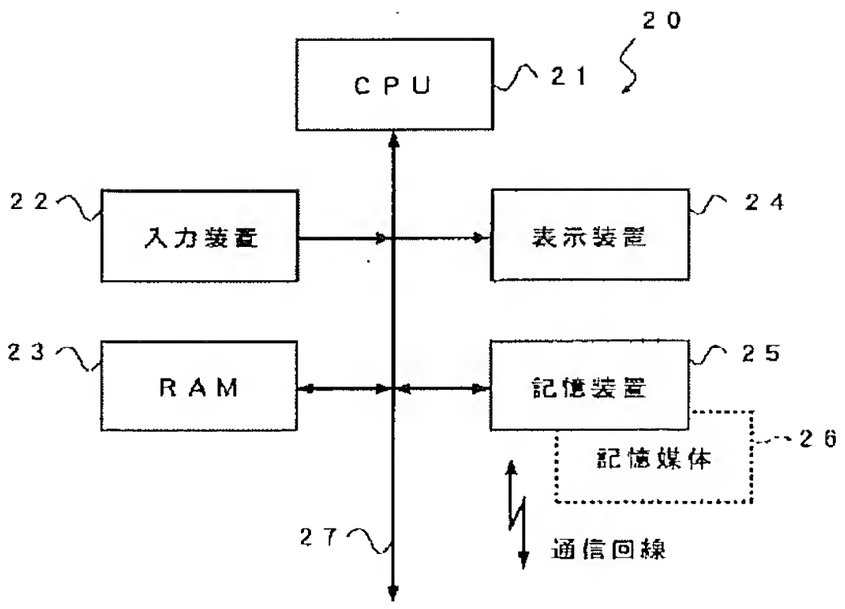
【図３】



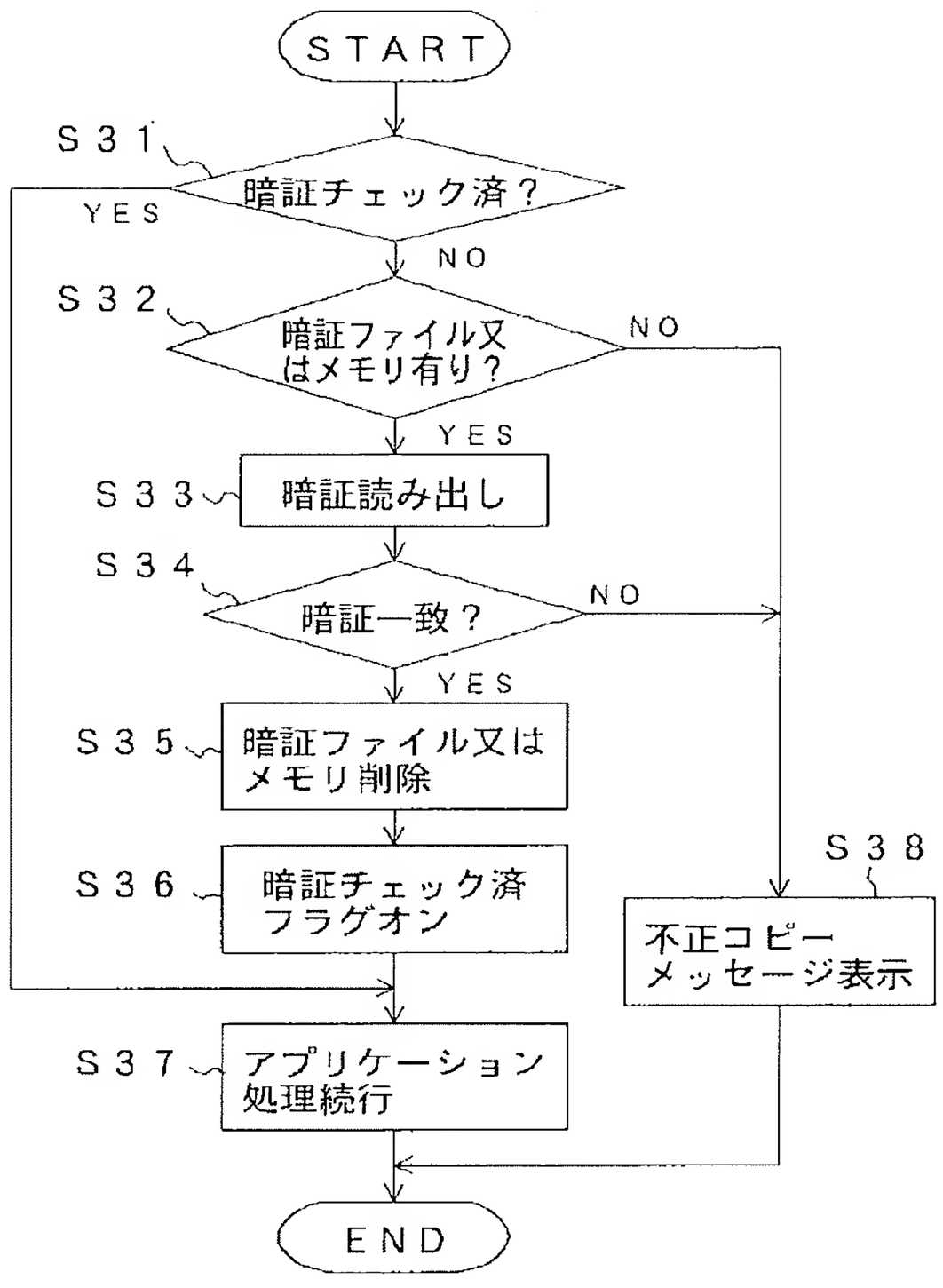
【図５】



【図４】


20
CPU
21
22
入力装置
表示装置
24
23
RAM
記憶装置
25
記憶媒体
26
27
通信回線

【図６】


START
S31
暗証チェック済？
YES
NO
S32
暗証ファイル又はメモリ有り？
NO
YES
S33
暗証読み出し
S34
暗証一致？
NO
YES
S35
暗証ファイル又はメモリ削除
S36
暗証チェック済フラグオン
S38
不正コピーメッセージ表示
S37
アプリケーション処理続行
END

The English Computer Translation (provided by the JPO) of Japanese Laid-Open Patent Publication No. 10-187433

CLAIMS

[Claim(s)]
[Claim 1]An electronic device which installs and uses an application program, comprising:
A code information storage means which stored beforehand peculiar code information which said application program sets up peculiar code information, and is set as this application program.
Peculiar code information set as the application program concerned when executing said application program.
A discriminating means which distinguishes whether it is a thing with the regular application program concerned by comparing peculiar code information stored in said code information storage means.
A control means which forbids execution of the application program concerned when said application program was not regular and it is distinguished as a result of this distinction.

[Claim 2]An electronic device which installs and uses an application program, comprising:
A memory measure which said application program has peculiar code information, and has a code file which memorizes code information corresponding to peculiar code information on this application program.
A code information collation means which compares existence and said peculiar code information on a code file within said memory measure when said application program is started first, When a code file exists and code information is in agreement as a result of this collation, A control means which executes the application program concerned based on existence of setting out of said code finishing information when said code file is eliminated and said application program is started henceforth, while setting up code finishing information.

[Claim 3]A storage which stored a program which can perform a computer, comprising:
Peculiar code information set as the application program concerned when executing an application program.
By comparing peculiar code information stored in a predetermined memory measure, A program code which can perform a computer for the application program concerned to distinguish whether it is a regular thing, A program code which can perform a computer for forbidding execution of the application program concerned when said application program was not regular and it is distinguished as a result of this distinction.

[Claim 4]It is the storage which stored a program which can perform a computer, A program code which can perform a computer for comparing coincidence with code information that it is peculiar to existence and said application program of a code file memorized by predetermined memory measure when an application program is started first, and a result of this collation, When a code file exists and code information is in agreement, While setting up code finishing information, when said code file is eliminated and said application program is started henceforth, A storage storing a program containing a program code which can perform a computer for executing the application program concerned based on existence of setting out of said code finishing information.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the electronic device and storage which prevent the illegal copy of software.
[0002]
[Description of the Prior Art]In the computer system which installs and uses software, such as the conventional application program, the typical technique which is described below is taken as a copy prevention method which prevents the illegal copy of the software.
** Format a master disk by a special file format, and prevent from creating a replica.
** Rewrite the contents of the master disk at the time of installation of software, and keep the copy more than the number of times of specification from being made.
** Input the password opened only to the registered user, when a password is not in agreement, the software does not operate, or keep continuation of installation from being possible at the time of installation of software.
[0003]
[Problem to be solved by the invention]However, since the master disk or the password suited under management of an end user if it was in the anti-copying method of such conventional software, there was a problem that a replica will be able to be easily created according to a user's morals.
[0004]Namely, though formatted by the file format with a special master disk, When it is easy to copy to a disk besides with the format form, and to create a duplicated disk and it inputs a password, If a registered user teaches the others a password, it is easy for the others other than a registered user to install software by a master disk.
[0005]For this reason, the above-mentioned conventional copy prevention method was not enough as the portion depending on a registered user's morals as a method of existing mostly and protecting software from an illegal copy.
[0006]It is the problem of this invention having a specific password on both sides with the hardware side which installs software the storage side which stores software, and checking coincidence of a password on both sides at the time of installation, It is giving the setting-out authority of a password to the system side, making the contents of the password a user with disclosure, and preventing the illegal copy of software.
[0007]
[Means for solving problem]The invention according to claim 1 equips with the following the electronic device which installs and uses an application program.
The code information storage means which stored beforehand the peculiar code information which said application program sets up peculiar code information, and is set as this application program.
Peculiar code information set as the application program concerned when executing said application program.
By comparing the peculiar code information stored in said code information storage means, The control means which forbids execution of the application program concerned when said application program was not regular and it is distinguished from the discriminating means from which the application program concerned distinguishes whether it is a regular thing as a result of this

distinction.

[0008]By therefore, the thing for which it has a specific password on both sides with the hardware side which installs software the storage side which stores software, and coincidence of a password is checked on both sides at the time of installation. The setting-out authority of a password can be given to the system side, the contents of the password can be made a user with disclosure, use of the application program in other computer systems can be prevented, and the illegal copy of the software by a user can be prevented.
[0009][0009]. Invention of ** installs an application program and a claim prepares the following for use.
Code file **** which said application program has peculiar code information, and memorizes code information corresponding to peculiar code information on this application program in a vessel.
A code which compares existence and said peculiar code information on a code file within said memory measure with a memory measure when said application program is started first.
When a code file exists and code information is in agreement a collation means and as a result of this collation, While setting up code finishing information, when said code file is eliminated and said application program is started henceforth, the application program concerned is executed based on existence of setting out of said code finishing information.

[0010]Therefore, by the software side, have a code file containing a specific password and at the time of application starting. Since a flag checked [code] is only checked and setting-out authority of a password was given to the software side, Even if a password is known by user, use of an application program copied illegally can be prevented being able to use to input a password after installation as meaningless.
[0011]
[Mode for carrying out the invention]Hereafter, with reference to figures, an embodiment of the invention is described in detail.
[0012](A 1st embodiment) Drawing 1 - drawing 3 are the figures showing the computer system of a 1st embodiment that applied the electronic device and storage of this invention.
[0013]First, composition is explained.
[0014]Drawing 1 is a block diagram showing the important section composition of the computer system 1 of a 1st embodiment. In this drawing 1, the computer system 1 is constituted by CPU2, the input device 3, RAM4, the display device 5, the code storing memory 6, the memory storage 7, and storage 8 grade, and each part except the storage 8 is connected to the bus 9.
[0015]CPU(Central Processing Unit) 2, The application program specified out of the SHITEMU program memorized by the memory storage 7 and the various application programs corresponding to the system concerned is stored in the program storage area in RAM4 which is not illustrated, While performing various processing according to the application program which stored in RAM4 the various directions or data inputted from the input device 3, and was stored in the memory storage 7 according to this input directions and input data and storing that processing result in RAM4, it displays on the display device 5. And the processing result stored in RAM4 is saved in the preservation destination in the memory storage 7 by which input directions are carried out from the input device 3.
[0016]When CPU2 performs the application process based on the application program mentioned later, The password first stored in the code storing memory 6 beforehand at the time of installation of an application program, Coincidence with the password beforehand set to the application program side is checked, When coincidence is checked, it judges that he is a registered user and an application process is continued, when not in agreement, it judges that it is an illegal copy and an illegal copy message is displayed on the display device 5, and an application process is stopped.
[0017]The input device 3 is provided with a cursor key, a number input key, a various function key, etc., and outputs a depression signal of a pressed key to CPU2.
[0018]RAM(Random Accesss Memory) 4 forms a memory area which stores temporarily a program processed by CPU2 and data. The display device 5 is constituted by CRT (Cathode Ray Tube) etc., and it displays a message which shows that it is an illegal copy inputted on the occasion of an

application process performed by the above-mentioned CPU2 while it displays an indicative data inputted from CPU2.
[0019]The code storing memory 6 is constituted by flash memory etc., and stores a password referred to when an application process is performed by the above-mentioned CPU2. A password stored in this code storing memory 6 is secretly stored in an end user beforehand, and makes access by a user improper.
[0020]The memory storage 7 has a program, data **, or the storage 8 memorized beforehand, and comprises that this storage 8 is magnetic, an optical recording medium, or semiconductor memory. This storage 8 is a thing provided in the memory storage 7 fixed, or a thing with which it equips enabling free attachment and detachment, To this storage 8, data etc. which were processed with the above-mentioned system program and various application programs corresponding to the system concerned, a password check processing program, and each processing program are memorized.
[0021]A program, data, etc. which are memorized to this storage 8, It may have composition received and memorized from other apparatus connected via a communication line etc., memory storage which equipped with the above-mentioned storage further other apparatus side connected via a communication line etc. may be formed, and it may have a program memorized by this storage 8 and composition which uses data via a communication line.
[0022]Next, operation of a 1st embodiment is explained.
[0023]An application process performed by the above-mentioned CPU2 is explained based on a flow chart shown in drawing 2.
[0024]If the storage 8 with which an application program was stored is set in the memory storage 7 and installs the application program in RAM4, CPU2, First, a password (XXXX--) beforehand set as this installed application program is read (Step S1), and password check function processing is performed (Step S2).
[0025]Details of this password check function processing are explained based on a flow chart shown in drawing 3.
[0026]In password check function processing shown in drawing 3, if developed by RAM4, a password (XXXX--) beforehand set as an application program, A password stored in the code storing memory 6 is read (Step S21), and it is distinguished whether a password set as the application program and a password read from the code storing memory 6 are in agreement (Step S22). Information on a purport that a password was in agreement when a password was in agreement is set up (Step S23), and it returns to Step S3 of drawing 2, and when a password is inharmonious, a password sets up information on an inharmonious purport (Step S24), and returns to Step S3 of drawing 2.
[0027]After this password check function processing is completed, it returns to Step S3 of drawing 2, and it is confirmed whether coincidence information on a password was set up, or nonconformity information was set up. he is a registered user when coincidence information on a password is set up, [judge and] When installation processing of an application program is continued (step S4) and nonconformity information of a password is set up, It judges that an installed application program is copied illegally and a message which shows that it is an illegal copy is displayed on the display device 5 (Step S5).
[0028]And after ending processing by an application program in step S4, or after ending display processing of an illegal copy message in Step S5, this application process is ended.
[0029]As mentioned above, in the computer system 1 of a 1st embodiment. When it has the code storing memory 6 which comprised a flash memory, a secret password is beforehand stored in this code storing memory 6 at an end user and an application process is performed, By checking coincidence with a password stored in this code storing memory 6, and a password set as an application program, Judging whether a set application program is a registered user's thing, and having judged [which continues the application program / or or] whether it would stop by the computer system 1 side A sake, Execution of an application program with which passwords copied illegally differ is avoidable.
[0030]By therefore, a thing for which it has a specific password on both sides with the hardware side which installs software the storage side which stores software, and coincidence of a password is checked on both sides at the time of installation. Setting-out authority of a password can be given to the system side, a user can write the contents of the password with disclosure, use of an application

program in other computer systems can be prevented, and an illegal copy of software by a user can be prevented.
[0031]Access by a user to the code storing memory 6 can be written as it is improper, a password can be prevented from preventing extraction of a password by a user and being known by user, and an illegal copy of an application program by acquisition of a password can be prevented.
[0032]When a password stored in the computer system 1 and a password set as an application program are in agreement in a 1st embodiment, execution of an application program is written as it is possible, As for the system configuration, it is more effective to apply to a computer system etc. which comprised a general-purpose thing in order to perform specific processing of paperwork etc. for example.
[0033]In a 1st embodiment, in order to prevent the illegal copy of software, stored the password in the code storing memory 6 which comprised a flash memory, but. The storing position of the password may be the same memory area as the memory area in the memory storage 7 with which software is installed, and the storing position in particular of a password is not limited.
[0034](A 2nd embodiment) Drawing 4 - drawing 6 are the figures showing the computer system of a 2nd embodiment that applied the electronic device and storage of this invention.
[0035]First, composition is explained.
[0036]Drawing 4 is a block diagram showing the important section composition of the computer system 20 of a 2nd embodiment. In this drawing 4, the computer system 20 is constituted by CPU21, the input device 22, RAM23, the display device 24, the memory storage 25, and storage 26 grade, and each part except the storage 26 is connected to the bus 27.
[0037]CPU(Central Processing Unit) 21, The application program specified out of the SHITEMU program memorized by the memory storage 25 and the various application programs corresponding to the system concerned is stored in the program storage area in RAM23 which is not illustrated, The various directions or data inputted from the input device 22 is stored in RAM23, While performing various processing according to the application program stored in the memory storage 25 according to this input directions and input data and storing that processing result in RAM23, it displays on the display device 24. And the processing result stored in RAM23 is saved in the preservation destination in the memory storage 25 by which input directions are carried out from the input device 22.
[0038]When CPU21 performs the application process based on the application program mentioned later, A code file is installed simultaneously with installation of the application program of RAM23, A password is stored in the code file memory 23a in RAM23, and other memory areas, respectively, Compare the existence and the contents (password) of a code file at the time of starting of this installed application program, and when in agreement, the code check flag 23c is set in RAM23 (ON), After eliminating a code file, only when the code check flag 23c is set (ON), continuation of processing of an application program is enabled.
[0039]The input device 3 is provided with a cursor key, a number input key, a various function key, etc., and outputs the depression signal of the pressed key to CPU2.
[0040]RAM(Random Accesss Memory) 23, While forming the memory area which stores temporarily the program processed by CPU21 and data, The code file memory 23a, the application program memory 23b, and checked [code] flag memory 23c ** which are shown in drawing 5 as a memory area in connection with an application process are formed. Since the code file installed with an application program on the occasion of the application process by the above-mentioned CPU21 is stored, the code file memory 23a is used, Since the application program installed is stored, the application program memory 23b is used. Since the flag turned on when collation of the contents of a code set by the code file installed on the occasion of the application process by the above-mentioned CPU21 is in agreement checked [code] is stored, the flag memory 23c checked [code] is used.
[0041]The display device 24 is constituted by CRT (Cathode Ray Tube) etc., and it displays the message which shows that it is an illegal copy inputted on the occasion of the application process performed by the above-mentioned CPU21 while it displays the indicative data inputted from CPU21.
[0042]The memory storage 25 has a program, data **, or the storage 26 memorized beforehand, and comprises that this storage 26 is magnetic, an optical recording medium, or semiconductor memory. This storage 26 is the thing provided in the memory storage 25 fixed, or a thing with which it equips

enabling free attachment and detachment, To this storage 26, the data etc. which were processed with the above-mentioned system program and the various application programs corresponding to the system concerned, a password check processing program, and each processing program are memorized.
[0043]A program, data, etc. which are memorized to this storage 26, It may have composition received and memorized from other apparatus connected via the communication line etc., The memory storage which equipped with the above-mentioned storage other apparatus side connected via the communication line etc. may be formed, and it may have program memorized by this storage 26 and composition which uses data via a communication line.
[0044]Next, operation of a 2nd embodiment is explained.
[0045]The application process performed by the above-mentioned CPU21 is explained based on the flow chart shown in drawing 6.
[0046]If the storage 26 with which the application program was stored is set in the memory storage 25 and starts installation of the application program, CPU21, First, it is confirmed whether the flag checked [code] is set to the flag memory 23c in RAM23 checked [code] (ON) (Step S31). When the flag checked [code] is set (ON), When processing of the application program shifted and installed in Step S37 is continued and the flag checked [code] is not set (OFF), It is confirmed whether the password is stored in each of the code file memory 23a in RAM23, or other memory areas (Step S32).
[0047]When the password is not stored in each of the code file memory 23a in RAM23, or other memory areas, It judges that the installed application program is copied illegally, shifts to Step S38, the message which shows that it is an illegal copy is displayed on the display device 24, and this application process is ended. When the password is stored in each of the code file memory 23a in RAM23, or other memory areas, it is confirmed whether read each of that password (Step S33), and each of that password is in agreement (Step S34).
[0048]When each of that read password is not in agreement, it shifts to Step S38, a message which shows that it is an illegal copy is displayed on the display device 24, and this application process is ended. When each of that read password is in agreement, A password is deleted to each of the code file memory 23a in RAM23, or other memory areas (Step S35), and a flag checked [code] is set to the flag memory 23c in RAM23 checked [code] (Step S36). (ON)
[0049]Subsequently, after continuing processing by an installed application program (Step S37) and ending processing by the application program, this application process is ended.
[0050]As mentioned above, in the computer system 20 of a 2nd embodiment. A code file which contains a password provided by an application program at the time of installation of an application program is set in RAM23, The code store file 6 needed by a 1st embodiment of the above is written as it is unnecessary, and it becomes possible to apply this invention also to a computer system of general composition.
[0051]After collation of the contents of a code deletes the code file and password, checks only a flag checked [code], and writes processing of the same application program as it is possible, Once starting an application program, installation of an application program including a code file copied illegally can be eliminated.
[0052]Therefore, by the software side, have a code file containing a specific password and at the time of application starting. Since the flag checked [code] is only checked and the setting-out authority of the password was given to the software side, Even if a password is known by the user, use of the application program copied illegally can be prevented being able to use to input a password after installation as meaningless. Use of the application program in other computer systems can be prevented like a 1st embodiment of the above, and the illegal copy of the software by a user can be prevented.
[0053]In order that after the end of installation may eliminate a code file, it becomes meaningless [access by the user to the code file 23a in RAM23], A password can be prevented from preventing extraction of the code file by a user and being known by the user, and the illegal copy of the application program by acquisition of a password can be prevented.
[0054]It is also possible to invisible-file-ize the code file itself, or to encipher the code file memory 23a, and to strengthen the measure against an illegal copy with a 2nd embodiment of the above.

[0055]
[Effect of the Invention]According to the electronic device of the invention according to claim 1, and the storage of the invention according to claim 3. By having a specific password on both sides with the hardware side which installs software the storage side which stores software, and checking coincidence of a password on both sides at the time of installation. The setting-out authority of a password can be given to the system side, the contents of the password can be made a user with disclosure, use of the application program in other computer systems can be prevented, and the illegal copy of the software by a user can be prevented.
[0056]According to the electronic device of the invention according to claim 2, and the storage of the invention according to claim 4, by the software side, have a code file containing a specific password and at the time of application starting. Since the flag checked [code] is only checked and the setting-out authority of the password was given to the software side, Even if a password is known by the user, use of the application program copied illegally can be prevented being able to use to input a password after installation as meaningless.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The block diagram showing the important section composition of the computer system of a 1st embodiment that applied the electronic device and storage of this invention.
[Drawing 2]The flow chart of the application process performed by CPU2 of drawing 1.
[Drawing 3]The flow chart of password check function processing of drawing 2.
[Drawing 4]The block diagram showing the important section composition of the computer system of a 2nd embodiment that applied the electronic device and storage of this invention.
[Drawing 5]The figure showing the memory configuration in RAM23 of drawing 4.
[Drawing 6]The flow chart of the application process performed by CPU21 of drawing 4.
[Explanations of letters or numerals]
1 and 20 Computer system
2, 21 CPU
3 and 22 Input device
4, 23 RAM
23a Code file memory
23b Application program memory
23c The flag memory checked [code]
5 and 24 Display device
6 Code storing memory
7 and 25 Memory storage
8 and 26 Storage
9 and 27 Bus

[Translation done.]